EXHIBIT F

Edit Details

Keywords:	E-mail Modems Fax lines
Responsible for contents:	022-23410
Version:	1
Published:	08/27/2004

Internet Use

WestLB's Internet access services are considered to be the property of the Bank and are to be used primarily for business purposes. WestLB reserves the right to monitor Internet usage by its employees. Personal use of the Internet, if it is infrequent and brief in duration and does not interfere in any way with job performance, is permitted. Excessive or improper use of the system may result in legal claims against both the employee and the Company and may result in disciplinary action up to and including termination of the offending employee. Consequently, the Bank expects that employees will use the Internet in a responsible and professional manner.

General guidelines to be observed include the following:

- WestLB's Internet services may not be used to solicit any commercial ventures, religious or political causes, outside organizations, or other non-job related solicitations.
- Access to offensive web sites is prohibited. Offensive sites include those that contain sexual connotations, racial slurs, gender-specific comments, or any other comment that offensively addresses someone's age, gender, sexual orientation, religious or political beliefs, national origin, or disability.
- Users are specifically prohibited from downloading programs, images, movies, documents, or any other materials from the Internet without gaining prior approval from the Information Security Officer. In no case will employee installation of software downloaded from the Internet be tolerated.
- All materials downloaded from the Internet (with approval) must be quarantined and virus scanned by Information Technology prior to being loaded on a WestLB network-connected computer.
- Users should be aware that when accessing the Internet using addresses and domain names registered to WestLB, they may be perceived by others as representing the Bank. Therefore, employees are advised not to use the Internet for any purpose or in any way that would reflect negatively on WestLB.

Employees who discover a violation to this policy are responsible for notifying the Information Security Officer immediately.

Electronic Mail

WestLB recognizes that electronic mail (e-mail) has become an essential tool for the conduct of business. However, improper use of this facility can result in liability to employees and the Bank. Consequently, all e-mail users are required to observe the following guidelines:

- The WestLB e-mail system should be used primarily for Bank related business only and not for personal or non-job related reasons.
- Occasional personal use of e-mail which does not interfere with an employee's job performance

and which is consistent with other Bank policies and guidelines is permitted.

- The WestLB e-mail system may not be used in connection with any trade or business in which the employee may engage outside of the Bank.
- All e-mail communications that pass through the WestLB system are the property of the Bank.
- Employees are prohibited from transmitting, retrieving or storing any communication of a discriminatory, defamatory, obscene, threatening, harassing or unlawful nature.
- Employees should not expect nor does the Bank assure the privacy or confidentiality of communications initiated from or received through the Bank's e-mail system.
- The Bank reserves the right to monitor, print and save all messages within its e-mail system to ensure adherence to Bank policies and protection of the Bank's intellectual property.
- Employees may not use e-mail to disclose confidential or proprietary information about or belonging to the Bank or for any purpose that is illegal, against Bank policy or contrary to the Bank's interest.
- Use of an employee e-mail account by anyone other than the account owner is forbidden.
- All messages sent to external (i.e., non-WestLB) recipients must have a suitably worded disclaimer appended.

Employees are expected to read, understand and abide by guidelines for the acceptable use of the WestLB e-mail system as set forth in Manual 130 and in further detail, in the Compliance database accessible through the WestLB NY Intranet.

Personally Owned E-mail Accounts

Employees and others whose services are retained by WestLB must refrain from initiating work-related communications, or discussing matters (or expressing opinions) pertaining to WestLB business or operations when using non-Bank (i.e., personal) electronic mail accounts (e.g., those provided by Yahoo!, Hotmail, home ISP, etc.). Business-related electronic communication should be conducted exclusively utilizing messaging services provided by and under the control of the Bank.

Unauthorized Use of Wireless Technology

The installation of wireless networking technology (e.g., 802.11b, 802.11a, 802.11g, "Bluetooth") on WestLB-provided computing equipment, whether stand-alone or networked, without gaining prior written authorization from IT management is prohibited. This includes the installation of wireless networking cards internally within desktop/tower workstations, through PCMCIA card slots on laptops or by means of usb or "firewire" connection on either.

Use of Modems

The installation and use of analog modems introduces significant security vulnerabilities to any computer network. The deployment of modems must be strictly controlled. A compelling business justification must be presented to IT before the use of such devices (whether in a workstation or a portable computing devices) will be approved. In those instances in which modem installation is deemed appropriate, only approved secure methods of connecting to the WestLB network (i.e., through RAS) or other resources may be used.

In those instances in which the installation of a modem has been approved (or in those cases where a modem is part of the computer's standard configuration as with laptops), policy prohibits its use to connect to any form of external service provider while the computer to which it is connected is simultaneously logged in to the WestLB network.

Finally, devices (primarily laptop computers) authorized to establish "dial-up" (i.e., "modem") connections to non-WestLB Internet Service Providers (ISPs) must have suitable firewall software

installed, configured, and active.

Use of Analog FAX Lines

Access to and use of analog telephone lines installed in support of facsimile (i.e., "Fax") machines must be controlled. Consequently, the use of these lines for any purpose other than fax support is prohibited. Specifically, the disconnecting of fax lines with the intention of reconnecting them to workstation- or laptop-installed modems is forbidden. Consultants, contractors and others who do not have access to the WestLB network and, therefore, require the use of an analog line to dial-in to their employer's system or other remote resource should direct a request for such a line to the person to whom they report.

Connection of Non-WestLB Equipment to the Network

Under no circumstance are employees, vendors, consultants or other individuals permitted to connect non-WestLB owned/configured computing equipment (i.e., personal laptops) to the WestLB local area network (LAN) without having obtained prior approval of IT management.

Remote Access to WestLB Systems

Employees, contractors, consultants, and others with a recognized need to access the WestLB internal network from remote locations (e.g., home, vendor premises, etc.) may do so only by means of the Bank's secure remote access solution (RAS). This solution should, at minimum:

- Provide for the encryption of data traversing the connection through the implementation of a VPN (virtual private network) or equivalent
- Require users to login to the system utilizing a two-factor authentication scheme (e.g., "SecurID").
- Require the installation and use of personal firewall software on all RAS-enabled computing devices.

Only WestLB-provided or certified client-side equipment may be used to access the WestLB network. Client software required to support a secure connection to WestLB must be installed and configured by IT personnel.

Modems used to provide dial-in capability to vendors for purposes of system support must be logically disabled or physically turned off when not needed. Only IT management or the CIO can authorize the re-enabling of these devices.

Instant Messaging

The installation or use of "instant messaging" programs by WestLB employees or others with access to WestLB computing equipment without the knowledge and consent of IT management is strictly forbidden.

Workflow History